РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ОТКРЫТЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ

20/43/2

Одобрено кафедрой
«Вычислительная техника»

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Задание на контрольную работу
с методическими указаниями
для студентов V курса
специальности

220100 Вычислительные машины, комплексы, системы и сети (ЭВМ)

Москва – 2005

Составитель — канд. техн. наук, доц. А.Е. Ермаков

Рецензент — д-р техн. наук, проф. В.Ю. Горелик

1. ЗАДАНИЕ НА КОНТРОЛЬНУЮ РАБОТУ

1.1. Общие требования к выполнению контрольной работы

Контрольная работа выполняется на листах формата А4. На титульном листе должны быть указаны данные студента и его учебный шифр. В контрольной работе должны быть выполнены все пункты задания, которое приводится в начале работы. Контрольные работы, не соответствующие указанным требованиям, возвращаются студенту без рецензии.

1.2. Исходные данные

С помощью симметричного криптографического алгоритма DES зашифровать свою фамилию, представленную в двоичном коде. Тип кодировки (приложение) определяется в соответствии с табл. 1. В качестве исходного ключа шифрования берется представленное в двоичном коде имя студента.

Таблица 1

Последняя цифра шифра	0	1	2	3	4	5	6	7	8	9
Тип кодировки	Unicod	win-1251	КОИ8	CP866	ISO8859-5	ISO8859-5	CP866	КОИ8	win-1251	Unicod

Примечание. При представлении символов кириллицы в двоичном коде рекомендуется использовать два последних шестнадцатеричных символа, приведенных в таблице приложения. Если разрядность полученного двоичного числа будет меньше 64 бит, то его следует дополнить в старшей части нулями.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ВЫПОЛНЕНИЮ КОНТРОЛЬНОЙ РАБОТЫ

2.1. Описание алгоритма DES

Алгоритм DES предназначен для шифрования 64-битовых блоков данных с помощью 64-битового ключа, в котором значащими являются 56 бит (остальные 8 бит — проверочные биты для контроля на четность). Дешифрование в DES является

операцией, обратной шифрованию, и выполняется путем повторения операций шифрования в обратной последовательности. Обобщенная схема процесса шифрования в алгоритме DES показана на рис.1. Процесс шифрования заключается в начальной перестановке битов 64-битового блока, шестнадцати циклах шифрования и, наконец, в конечной перестановке битов.

При описании алгоритма DES применены следующие обозначения:

- L и R — последовательности битов (левая (left) и правая (right));
- LR — конкатенация последовательностей L и R, т.е. такая последовательность битов, длина которой равна сумме длин L и R; в последовательности LR биты последовательности R следуют за битами последовательности L;
- $\oplus$ — операция побитового сложения по модулю 2.

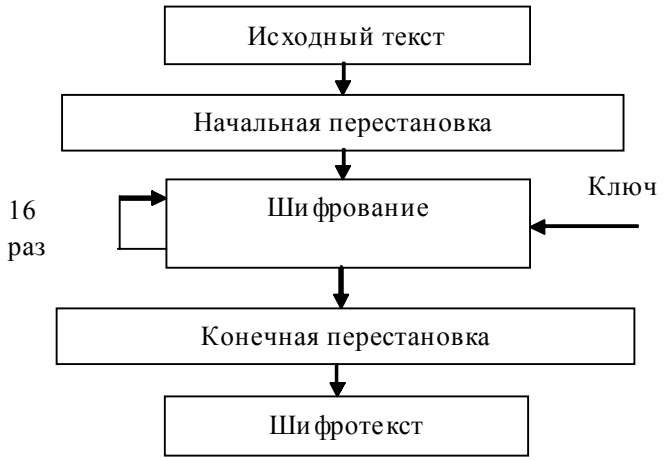

Рис.1. Обобщенная схема шифрования в алгоритме DES

Блок-схема алгоритма DES приведена на рис. 2. Пусть из файла исходного текста считан очередной 64-битовый (8-байтовый) блок T. Этот блок T преобразуется с помощью *матрицы начальной перестановки* P (табл. 2).

Таблица 2

Матрица начальной перестановки P

		Номер бита							
		1	2	3	4	5	6	7	8
Номер байта	1	58	50	42	34	26	18	10	2
	2	60	52	44	36	28	20	12	4
	3	62	54	46	38	30	22	14	6
	4	64	56	48	40	32	24	16	8
	5	57	49	41	33	25	17	9	1
	6	59	51	43	35	27	19	11	3
	7	61	53	45	37	29	21	13	5
	8	63	55	47	39	31	23	15	7

Биты входного блока T (64 бита) переставляются в соответствии с матрицей P: бит 58 входного блока T становится битом 1, бит 50 — битом 2 и т.д. Эту перестановку можно описать выражением $T_0 = P(T)$. Полученная последовательность битов T_0 разделяется на две последовательности: L_0 — левые или старшие биты, R_0 — правые или младшие биты, каждая из которых содержит 32 бита.

Затем выполняется итеративный процесс шифрования, состоящий из 16 шагов (циклов). Пусть T_i — результат i-й итерации:

$$T_i = L_i R_i,$$

где $L_i = t_1 t_2 \ldots t_{32}$ (первые 32 бита);
$R_i = t_{33} t_{34} \ldots t_{64}$ (последние 32 бита).

Тогда результат i-й итерации описывается следующими формулами:

$$L_i = R_{i-1}, \quad i = 1, 2..., 16;$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i), \quad i = 1, 2..., 16;$$

Функция F называется функцией шифрования. Ее аргументами являются последовательность R_i, получаемая на предыдущем шаге итерации, и 48-битовый ключ K_i, который является результатом преобразования 64-битового ключа шифра K. (Подробнее функция шифрования F и алгоритм получения ключа K, описаны ниже.)

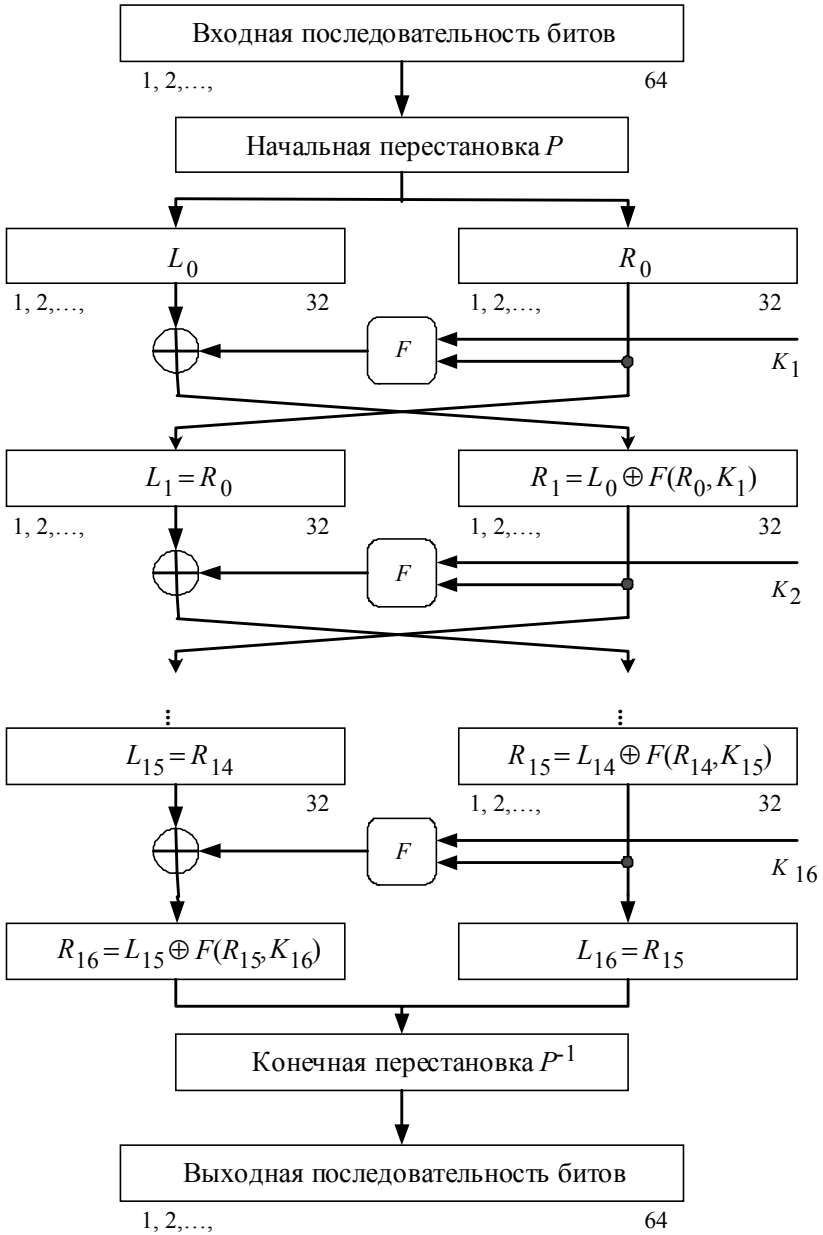

Рис. 2. Блок – схема алгоритма DES

На последнем шаге итерации получают последовательности R_{16} и L_{16} (без перестановки местами), которые конкатенируются в 64-битовую последовательность $R_{16}\,L_{16}$.

По окончании шифрования осуществляется восстановление позиций битов с помощью матрицы обратной перестановки P^{-1} (табл. 3).

Таблица 3

Матрица обратной перестановки P^{-1}

		Номер бита							
		1	2	3	4	5	6	7	8
Номер байта	1	40	8	48	16	56	24	64	32
	2	39	7	47	15	55	23	63	31
	3	38	6	46	14	54	22	62	30
	4	37	5	45	13	53	21	61	29
	5	36	4	44	12	52	20	60	28
	6	35	3	43	11	51	19	59	27
	7	34	2	42	10	50	18	58	26
	8	33	1	41	9	49	17	57	25

2.2. Вычисление функции шифрования

Схема вычисления функции шифрования $F\,(R_{i-1}K_i)$ показана на рис. 3. Для вычисления значения функции F используются:

- функция E (расширение 32 бит до 48);
- функции S_1, S_2, ... S_8 (преобразование 6-битового числа в 4-битовое);
- функция P (перестановка битов в 32-битовой последовательности).

Функция расширения E выполняет преобразование 32 битного числа R_{i-1} в 48 разрядное в соответствии с табл. 4. Как следует из табл. 4 первые три бита $E\,(R_{i-1})$ — это биты 32, 1 и 2, а последние — 31, 32, 1. Полученный результат (обозначим его $E\,(R_{i-1})$) складывается по модулю 2 с текущим значением ключа K_j и затем разбивается на восемь 6-битовых блоков (секстетов) B_1, B_2,..., B_8:

$$E\,(R_{i-1})\oplus K_i = B_1 B_2 \ldots B_8.$$

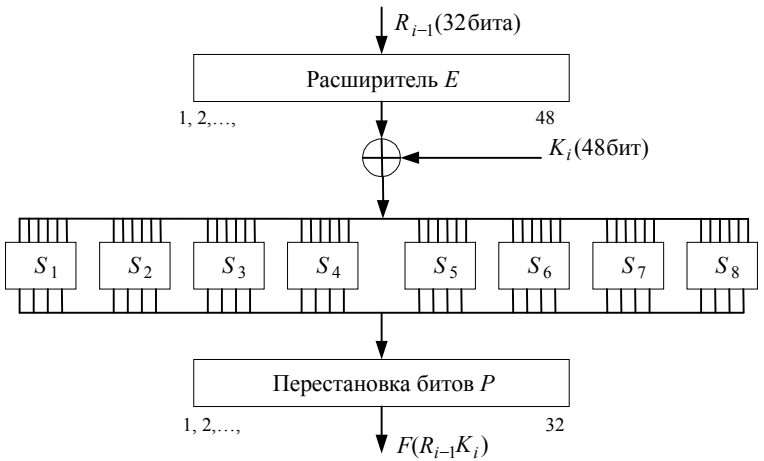

Рис. 3. Схема вычисления функции шифрования F

Таблица 4

Функция расширения E

		Номер бита					
		1	2	3	4	5	6
Номер секстета	1	32	1	2	3	4	5
	2	4	5	6	7	8	9
	3	8	9	10	11	12	13
	4	12	13	14	15	16	17
	5	16	17	18	19	20	21
	6	20	21	22	23	24	25
	7	24	25	26	27	28	29
	8	28	29	30	31	32	1

Далее каждый из этих блоков используется как номер элемента в функциях-матрицах S_1, S_2, ... S_8, содержащих 4-битовые значения (табл. 5).

Следует отметить, что выбор элемента в матрице S_j осуществляется достаточно оригинальным образом. Пусть на вход матрицы S_j поступает 6-битовый блок $B_j = b_1b_2b_3b_4b_5b_6$. Тогда двухбитовое число b_1b_6 указывает номер строки матрицы, а четырехбитовое число $b_2b_3b_4b_5$ — номер столбца. Например, если на вход матрицы S_1 поступает 6-битовый блок B_1 =100110,

Таблица 5

Функции преобразования S_1, S_2, ... S_8

		Номер столбца																
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Номер строки	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	S_1
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
	2	4	1	4	8	13	6	2	11	15	12	9	7	3	10	5	0	
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	S_2
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	S_3
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	S_4
	1	13	8	11	5	6	15	.0	3	4	7	2	12	1	10	14	9	
	2	10	6	-9	0	12	11	7	13	15	1	3	14	5	2	8	4	
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	S_5
	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
	3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	S_6
	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	1	6	
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	S_7
	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	S_8
	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

то 2-битовое число $b_1b_6 = 10_2 = 2_{10}$ указывает строку с номером 2 матрицы S_1, а 4-битовое число $b_2b_3b_4b_5 = 0011_2 = 3_{10}$ указывает столбец с номером 3 матрицы S_1. Это означает, что в матрице S_1 блок $B_1 = 100110$ выбирает элемент на пересечении строки с номером 2 и столбца с номером 3, т.е. элемент $8_{10} = 1000_2$. Совокупность 6-битовых блоков B_1, B_2, ... B_8 обеспечивает выбор четырехбитового элемента в каждой из матриц S_1, S_2, ... S_8.

В результате получаем $S_1(B_1)\ S_2(B_2)$ ... $S_8(B_8)$, т.е. 32-битовый блок (поскольку матрицы S_j содержат 4-битовые элементы). Этот 32-битовый блок преобразуется с помощью функции перестановки битов P (табл. 6).

Таблица 6

Функция P перестановки битов

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Таким образом, функция шифрования

$$F(R_{i-1},K_i) = P(S_1(B_1),...,S_8(B_8)).$$

2.3. Вычисление ключей шифрования

Как нетрудно заметить, на каждой итерации используется новое значение ключа K_i, (длиной 48 бит). Новое значение ключа K_i вычисляется из начального ключа K (рис.4). Ключ K представляет собой 64-битовый блок с 8 битами контроля по четности, расположенными в позициях 8, 16, 24, 32, 40, 48, 56, 64. Для удаления контрольных битов и подготовки ключа к работе используется функция G первоначальной подготовки ключа (табл.7).

Табл. 7 разделена на две части. Результат преобразования $G(K)$ разбивается на две половины C_0 и D_0 по 28 бит каждая. Первые четыре строки матрицы G определяют, как выбираются биты последовательности C_0 (первым битом C_0 будет бит 57 ключа шифра, затем бит 49 и т.д., а последними битами — биты 44 и 36 ключа).

Таблица 7

Функция Q первоначальной подготовки ключа битов (переставленная выборка 1)

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

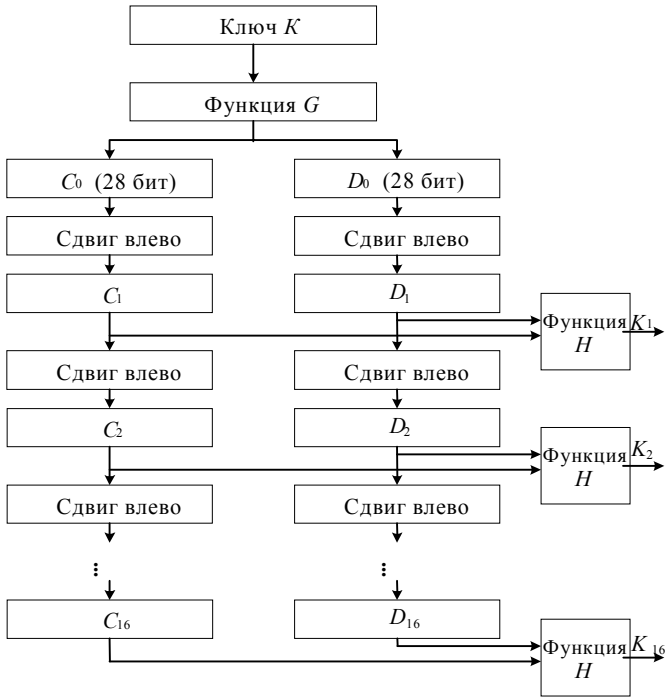

Рис. 4. Схема алгоритма вычисления ключей K

Следующие четыре строки матрицы G определяют, как выбираются биты последовательности D_0 (т.е. последовательность D_0 будет состоять из битов 63, 55, 47,...,12, 4 ключа шифра).

Как видно из табл. 7, для генерации последовательностей C_0 и D_0 не используются биты 8, 16, 24, 32, 40, 48, 56 и 64 ключа шифра. Эти биты не влияют на шифрование и могут служить для других целей (например, для контроля по четности). Таким образом, в действительности ключ шифра является 56-битовым.

После определения C_0 и D_0 рекурсивно определяются C_i и D_i, i = 1, 2,.... 16. Для этого применяются операции циклического сдвига влево на один или два бита в зависимости от номера шага итерации, как показано в табл. 8.

Операции сдвига выполняются для последовательностей C_i и D_i, независимо. Например, последовательность C_3 получается посредством циклического сдвига влево на две позиции последовательности C_2, а последовательность D_3 — посредством сдвига влево на две позиции последовательности D_2. Последовательности C_{16} и D_{16} получаются из C_{15} и D_{15} посредством сдвига влево на одну позицию.

Таблица 8

Таблица сдвигов S_i для вычисления ключа

Номер итерации	Количество сдвигов влево, бит		Номер итерации	Количество сдвигов влево, бит
1	1		9	1
2	1		10	2
3	2		11	2
4	2		12	2
5	2		13	2
6	2		14	2
7	2		15	2
8	2		16	1

Ключ K_i, определяемый на каждом шаге итерации, есть результат выбора конкретных битов из 56-битовой последовательности C_i, D_i и их перестановки. Другими словами, ключ, $K_i=H(C_iD_i)$, где функция H определяется матрицей, завершающей обработки ключа (табл. 9).

Таблица 9

Функция H завершающей обработки ключа (переставленная выборка 2)

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Как следует из табл. 9, первым битом ключа K_i, будет 14-й бит последовательности C_i, D_i, вторым — 17-й бит, 47-м битом ключа K_i будет 29-й бит C_i, D_i, а 48-м битом — 32-й бит C_i, D_i.

2.4. Расшифрование данных

Процесс расшифрования данных является инверсным по отношению к процессу шифрования. Все действия должны быть выполнены в обратном порядке. Это означает, что расшифровываемые данные сначала переставляются в соответствии с матрицей P^{-1}, а затем над последовательностью битов $R_{16}L_{16}$ выполняются те же действия, что и в процессе шифрования, но в обратном порядке.

Итеративный процесс расшифрования может быть описан следующими формулами:

$$R_{i-1} = L_i, \ i = 1, 2..., 16;$$

$$L_{i-1} = R_i \oplus F(L_i, K_i), \ i = 1, 2..., 16.$$

Таким образом, для процесса расшифрования с переставленным входным блоком $R_{16}L_{16}$ на первой итерации используется ключ K_{16}, на второй итерации — K_{15} и т.д. На 16-й итерации используется ключ K_1. На последнем шаге итерации будут получены последовательности L_0 и R_0, которые конкатенируются в 64-битовую последовательность L_0R_0. Затем в этой

последовательности 64 бита переставляются в соответствии с матрицей *P*. Результат такого преобразования — исходная последовательность битов (расшифрованное 64-битовое значение).

Поскольку процессы шифрования и расшифрования информации связаны с выполнением громоздких вычислений, выполняемых над двоичными числами, то рекомендуется их автоматизировать. С этой целью целесообразно составить программу (программы) на одном из языков высокого уровня. При этом текст программы должен быть приведен в приложении к контрольной работе.

ЛИТЕРАТУРА

1. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. —М.: Радио и связь, 2001. – 328 с.

2. Яковлев В.В., Корниенко А.А. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта: Учебник для вузов ж.д. транспорта. —М.: УМК МПС России, 2002. – 328 с.

3. ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

4. http://book.itep.ru

Таблица кодировки символов кириллицы

Unicode	win-1251	КОИ8	CP866	ISO8859-5		Unicode	win-1251	КОИ8	CP866	ISO8859-5	
0x0401	0xA8	0xB3	0xf0	0xA1	Ё	0x0430	0xE0	0xC1	0xa0	0xD0	а
0x0410	0xC0	0xE1	0x80	0xB0	А	0x0431	0xE1	0xC2	0xa1	0xD1	б
0x0411	0xC1	0xE2	0x81	0xB1	Б	0x0432	0xE2	0xD7	0xa2	0xD2	в
0x0412	0xC2	0xF7	0x82	0xB2	В	0x0433	0xE3	0xC7	0xa3	0xD3	г
0x0413	0xC3	0xE7	0x83	0xB3	Г	0x0434	0xE4	0xC4	0xa4	0xD4	д
0x0414	0xC4	0xE4	0x84	0xB4	Д	0x0435	0xE5	0xC5	0xa5	0xD5	е
0x0415	0xC5	0xE5	0x85	0xB5	Е	0x0436	0xE6	0xD6	0xa6	0xD6	ж
0x0416	0xC6	0xF6	0x86	0xB6	Ж	0x0437	0xE7	0xDA	0xa7	0xD7	з
0x0417	0xC7	0xFA	0x87	0xB7	З	0x0438	0xE8	0xC9	0xa8	0xD8	и
0x0418	0xC8	0xE9	0x88	0xB8	И	0x0439	0xE9	0xCA	0xa9	0xD9	й
0x0419	0xC9	0xEA	0x89	0xB9	Й	0x043A	0xEA	0xCB	0xaa	0xDA	к
0x041A	0xCA	0xEB	0x8a	0xBA	К	0x043B	0xEB	0xCC	0xab	0xDB	л
0x041B	0xCB	0xEC	0x8b	0xBB	Л	0x043C	0xEC	0xCD	0xac	0xDC	м
0x041C	0xCC	0xED	0x8c	0xBC	М	0x043D	0xED	0xCE	0xad	0xDD	н
0x041D	0xCD	0xEE	0x8d	0xBD	Н	0x043E	0xEE	0xCF	0xae	0xDE	о
0x041E	0xCE	0xEF	0x8e	0xBE	О	0x043F	0xEF	0xD0	0xaf	0xDF	п
0x041F	0xCF	0xF0	0x8f	0xBF	П	0x0440	0xF0	0xD2	0xe0	0xE0	р
0x0420	0xD0	0xF2	0x90	0xC0	Р	0x0441	0xF1	0xD3	0xe1	0xE1	с
0x0421	0xD1	0xF3	0x91	0xC1	С	0x0442	0xF2	0xD4	0xe2	0xE2	т
0x0422	0xD2	0xF4	0x92	0xC2	Т	0x0443	0xF3	0xD5	0xe3	0xE3	у
0x0423	0xD3	0xF5	0x93	0xC3	У	0x0444	0xF4	0xC6	0xe4	0xE4	ф
0x0424	0xD4	0xE6	0x94	0xC4	Ф	0x0445	0xF5	0xC8	0xe5	0xE5	х
0x0425	0xD5	0xE8	0x95	0xC5	Х	0x0446	0xF6	0xC3	0xe6	0xE6	ц
0x0426	0xD6	0xE3	0x96	0xC6	Ц	0x0447	0xF7	0xDE	0xe7	0xE7	ч
0x0427	0xD7	0xFE	0x97	0xC7	Ч	0x0448	0xF8	0xDB	0xe8	0xE8	ш
0x0428	0xD8	0xFB	0x98	0xC8	Ш	0x0449	0xF9	0xDD	0xe9	0xE9	щ
0x0429	0xD9	0xFD	0x99	0xC9	Щ	0x044A	0xFA	0xDF	0xea	0xEA	ъ
0x042A	0xDA	0xFF	0x9a	0xCA	Ъ	0x044B	0xFB	0xD9	0xeb	0xEB	ы
0x042B	0xDB	0xF9	0x9b	0xCB	Ы	0x044C	0xFC	0xD8	0xec	0xEC	ь
0x042C	0xDC	0xF8	0x9c	0xCC	Ь	0x044D	0xFD	0xDC	0xed	0xED	э
0x042D	0xDD	0xFC	0x9d	0xCD	Э	0x044E	0xFE	0xC0	0xee	0xEE	ю
0x042E	0xDE	0xE0	0x9e	0xCE	Ю	0x044F	0xFF	0xD1	0xef	0xEF	я
0x042F	0xDF	0xF1	0x9f	0xCF	Я	0x0451	0xB8	0xA3	0xf1	0xF1	ё

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Задание на контрольную работу
с методическими указаниями

Редактор *Д.Н. Тихонычев*
Корректор *В.В. Игнатова*
Компьютерная верстка *Ю.А. Варламова*

Тип. зак.	Изд. зак. 211	Тираж 900 экз.
Подписано в печать 14.02. 05	Гарнитура Times.	Офсет
Усл. печ. л. 1,0		Формат 60×90 1/16

Издательский центр РГОТУПСа,
125993, Москва, Часовая ул., 22/2

Участок оперативной печати РГОТУПСа, 125993, Москва, Часовая ул., 22/2